УДК 343. 9: 343. 346. 8

В. М. Воробей, 4 курс
Науковий керівник: Л. В. Раєцька,
кандидат юридичних наук, доцент,
професор кафедри кримінально-правових дисциплін
Навчально-науковий інститут права та психології
Національної академії внутрішніх справ (Україна)

ПРОБЛЕМИ ПОПЕРЕДЖЕННЯ ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ

В статье осуществлен анализ киберпреступлений и кибертерроризма, который составляет угрозу как отдельным гражданам, так и информационной безопасности государства, факторы и проблематику предупреждения киберпреступности в Украине.

Кіберзлочини – це суспільно-небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами.

Актуальність теми дослідження полягає у проблематиці попередження кіберзлочинності та підготовки кадрів у сфері інформаційних технологій і кібербезпеки. Це питання досить часто обговорюється фахівцями у сфері новітніх технологій, інформаційної безпеки та державного управління в журналах, на конференціях, круглих столах і засобах масової інформації, однак не дістало всебічного наукового дослідження [1].

Кіберзлочинність – це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера інформаційний, у якому перебувають відомості про особи, предмети, факти, подіях, явищах і процесах, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [2, с. 33].

Конвенція Ради Європи говорить про чотири типи комп'ютерних злочини «у чистому вигляді», визначаючи їх як злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем: 1) незаконний доступ – ст. 2 (протиправний умисний доступ до комп'ютерної системи або її частини); 2) незаконне перехоплення – ст. 3 (протиправне умисне перехоплення не призначених для громадськості передач комп'ютерних даних на комп'ютерну систему, з неї або в її межах); 3) втручання в дані – ст. 4 (протиправне ушкодження, видалення, порушення, зміна або припинення комп'ютерних даних); 4) втручання в

систему – ст. 5 (серйозна протиправна перешкода функціонуванню комп'ютерної системи шляхом введення, передачі, ушкодження, видалення, порушення, зміни або припинення комп'ютерних даних) [3].

Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова, а це означає що профілактичними заходами в даному випадку можуть бути дії спрямовані на регулярну перевірку рахунків тих, хто потрапляв хоч один раз в поле зору з даних питань.

Друга причина росту кіберзлочинності як бізнесу – те, що успіх справи не пов'язаний з великим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, будь то окремі люди або цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше.

Проблемою профілактики в даному випадку може бути неможливість передбачення та попередження «майбутніх» жертв про ймовірну небезпеку.

Кіберзлочинність – явище новітньої, цифрової доби. Саме це й робить «кіберів» набагато небезпечнішими й ефективнішими за своїх «класичних» колег-шахраїв.

Статистика свідчить, що наша країна є одним з лідерів за кількістю кібератак у всьому світі. Україна виявилася у цій сфері на четвертому місці після Росії, Тайваню і Німеччини [1].

Кібертероризм становлять загрозу як окремим громадянам, так і інформаційній безпеці держави. Інформаційна безпека є невід'ємною складовою національної безпеки і важливою самостійною сферою забезпечення національної безпеки [4, с. 80].

Для поліпшення ситуації необхідно проводити такі заходи: сформувати реєстр фахівців з боротьби з кіберзлочинністю з-поміж– управлінського апарату, науково-педагогічного складу, практичних працівників, випускників, що пройшли відповідну підготовку; за підсумками роботи міжвідомчого науково-практичного заходу,– куди необхідно притягнути провідних фахівців, має бути сформована робоча група з удосконалення державної стратегії боротьби з кіберзлочинністю; має бути прийняте управлінське рішення про системний розподіл– підготовки фахівців з цього напряму в конкретних ВНЗ за конкретними спеціалізаціями для слідчих, оперативних і експертних підрозділів; необхідно або усунути дублювання в роботі оперативних підрозділів – по боротьбі з кіберзлочинністю, або чітко встановити їх спеціалізацію; в ідеалі має бути створене самостійне Центральне Управління по – боротьбі з кіберзлочинністю в Україні [1].

На законодавчому рівні в Україні залишається невирішеними чимало питань у сфері протидії кіберзлочинності. Це насамперед, відсутність у вітчизняному законодавстві чіткого визначення поняття «кіберзлочинність». Визначення такого терміну може дати значний поштовх до приведення у відповідність інших законодавчих актів.

Список основних джерел

1. Державна політика підготовки кадрів з попередження кіберзлочинності в Україні [Електронний ресурс]. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/apdu/2014-1/doc/5/01.pdf. – Дата доступу: 12.05.2015.

2. Біленчук, Д. П. Кібрешахраї – хто вони? / Д. П. Біленчук // Міліція України. – 1999. – № 7–8. – С. 32–34.

3. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/994_575. – Дата доступу: 13.05.2015.

4. Тихомиров, О. О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки / О. О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., Київ, 22 берез. 2011 р. / НА СБ України. – Київ, 2011. – Ч. 2. – С. 78–82.

УДК 343.82

Д. А. Добров, 1 курс
Научный руководитель: Э. А. Юнусов,
кандидат юридических наук,
старший преподаватель кафедры теории государства
и права, международного и европейского права
Академии ФСИН России (Рязань)

ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ФЕНОМЕНА КОРРУПЦИИ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ

В работе рассматриваются теоретические вопросы понятия и сущности коррупции и проблемы противодействия коррупционным проявлениям в уголовно-исполнительной системе.

О важности проблемы коррупции не только в уголовно-исполнительной системе, но и в масштабах всей страны свидетельствуют многочисленные исследования в данной области, заседания высших органов государственной власти, главной целью которой является воспрепятствие этому злу путем выработ-